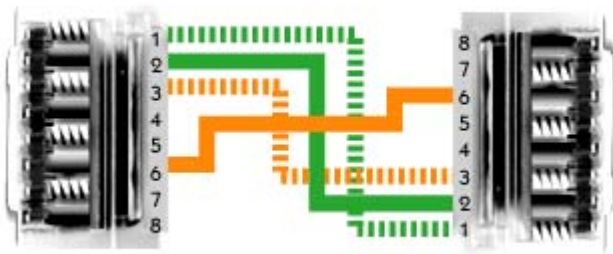
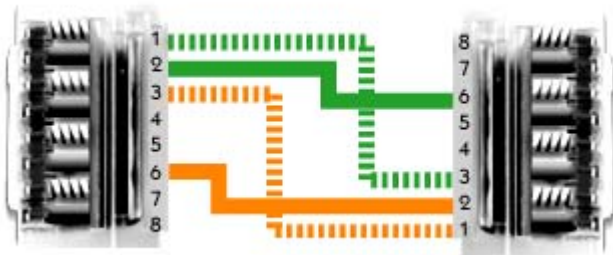


3.1. LAN Connection

When connecting devices in a LAN, you will need to use different types of Ethernet cables. You will need to know the pin positions of the cable types to differentiate them from each other.

The types of Ethernet cables used for LAN connections include the following:

Type	Pin Position	Uses
 Straight-through Ethernet Cable	1 --> 1 2 --> 2 3 --> 3 6 --> 6	Use a straight-through Ethernet cable when connecting the following devices: <ul style="list-style-type: none">• Workstation to hub• Workstation to switch• Router to hub• Router to switch
 Crossover Ethernet Cable	1 --> 3 2 --> 6 3 --> 1 6 --> 2	Use a crossover Ethernet cable when connecting the following devices: <ul style="list-style-type: none">• Switch to switch• Switch to hub• Hub to hub• Workstation to router• Workstation to workstation• Router to router

Be aware of the following when making LAN connections:

- Through Auto-MDI/MDIX, newer switches can determine what type of Ethernet cable is needed and will internally change the sending/receiving pin positions if needed.
- Some Cisco routers provide a generic Attachment Unit Interface (AUI) port. The AUI port is designed to connect to an external transceiver for conversion to a specific media type, such as coaxial or fiber optic.
- To support LAN distances above twisted pair Ethernet limits (>100 meters), use the switch's **SFP slot (Gigabit uplink port)** and **fiber optic media**.

3.2. Switch Activity

In this course, you will learn how to configure the Catalyst 2960 series switch. The 2960 series switch has various status lights (or LED's) which provide information about the switch's activity.

Light		Meaning
SYST (System)		<p>A single system light gives you information about the overall switch status.</p> <ul style="list-style-type: none">• Solid green = System is operational• Solid amber = System is receiving power but is not functioning properly• Off = System is not powered on
RPS (Redundant Power Supply)		<p>A single RPS light shows the status of the redundant power supply.</p> <ul style="list-style-type: none">• Solid green = RPS is present and ready to provide back-up power• Flashing green = RPS is connected, but is unavailable because it is providing power to another device• Solid amber = RPS is in standby mode or in a fault condition• Off = RPS is off or not properly connected
Port	Each port has a light that indicates the status of the port. By pressing the Mode button, you can view three different types of information for each port.	
	Stat (Port status)	<p>When the Mode button selects Stat:</p> <ul style="list-style-type: none">• Solid green = Link present and is operational• Flashing green = Link activity (port is sending or receiving data)• Alternating green-amber = Link fault (Error frames can affect connectivity, and errors such as excessive collisions,

		<p>cyclic redundancy check (CRC) errors, and alignment and jabber errors are monitored for a link-fault indication)</p> <ul style="list-style-type: none"> • Solid amber = Port is blocked by Spanning Tree Protocol (STP) and <i>is not</i> forwarding data • Flashing amber = Port is blocked by STP and <i>is</i> sending or receiving packets • Off = No link, or port was administratively shut down (if viewing the port status with the GUI, a brown color indicates a shutdown port)
	Duplex (Port duplex mode)	<p>When the Mode button selects Duplex:</p> <ul style="list-style-type: none"> • Solid green = Full duplex • Off = Half duplex, or no link present (if viewing the port duplex with the GUI, a blue color indicates half duplex)
	Speed (Port speed)	<p>When the Mode button selects Speed:</p> <ul style="list-style-type: none"> • Flashing green = 1000 Mbps (1 Gbps) • Solid green = 100 Mbps • Off = 10 Mbps, or no link present (if viewing the port speed with the GUI, a blue color indicates 10 Mbps)

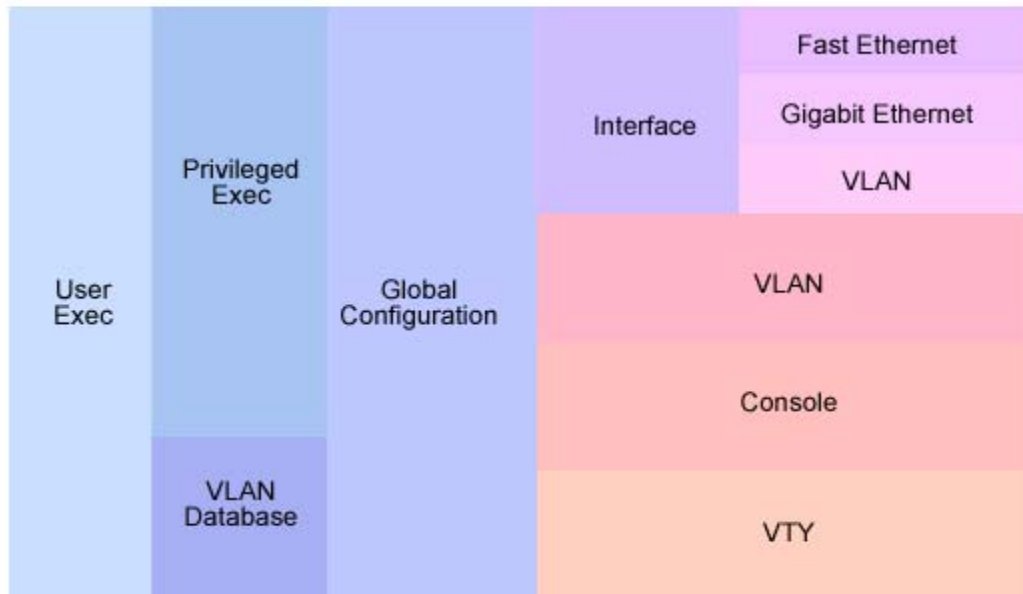
On a simple LAN, you can connect the switch to the network, connect devices, and it will automatically begin switching traffic to the correct ports. The switch comes preconfigured to work out-of-the-box without configuration. To customize the switch configuration, connect to the switch in one of the following ways:

- Console connection
- Telnet session
- Web management software (connect through the LAN through a Web browser)

Note: You must configure an IP address for the switch to manage it through a Telnet or Web session.

3.3. Switch Configuration Modes

The following graphic illustrates some of the configuration modes of the switch.



The following table describes some of the configuration modes of the switch:

Mode	Details	CLI Mode Prompt
Interface configuration	<p>The switch has multiple interface modes depending on the physical (or logical) interface type. For this course, you should be familiar with the following switch interface modes:</p> <ul style="list-style-type: none">Ethernet (10 Mbps Ethernet)FastEthernet (100 Mbps Ethernet)GigabitEthernet (1 GB Ethernet)VLAN <p>Note: The VLAN interface configuration mode is used to configure the switch IP address and other management functions.</p>	Switch(config-if)#

	<p><i>It is a logical management interface configuration mode, instead of a physical interface configuration mode as used for the FastEthernet and GigabitEthernet ports.</i></p>	
Config-vlan	<p>Details of the config-vlan mode include the following:</p> <ul style="list-style-type: none"> You can use the config-vlan mode to perform all VLAN configuration tasks. Changes made in vlan mode take place immediately. <p>Note: Do not confuse the config-vlan mode with the VLAN interface configuration mode.</p>	Switch(config-vlan)#
VLAN configuration	<p>Details of the VLAN configuration mode include the following:</p> <ul style="list-style-type: none"> The vlan configuration mode allows you to only configure a subset of VLAN features. Changes made in the VLAN configuration mode do not take effect until you save the changes, either before or while exiting the configuration mode. Changes made in the VLAN configuration mode are not stored in the regular switch configuration file. <p>Note: The 2960 switch recommends that you configure VLAN parameters from config-vlan mode, because VLAN configuration mode is being deprecated (phased out).</p>	Switch(vlan)#

Line configuration	Use this mode to configure parameters for the terminal line, such as the console, Telnet, and SSH lines.	<i>Switch(config-line)#</i>
---------------------------	--	------------------------------------

3.4. Switch Configuration Commands

The following table lists common switch configuration commands:

Task	Command
Move to interface configuration mode	<i>switch(config)#interface FastEthernet 0/14</i> <i>switch(config)#interface GigabitEthernet 0/1</i>
Move to configuration mode for a range of interfaces	<i>switch(config)#interface range fastethernet 0/14 - 24</i> <i>switch(config)#interface range gigabitethernet 0/1 - 4</i> <i>switch(config)#interface range fa 0/1 - 4, 7 - 10</i> <i>switch(config)#interface range fa 0/8 - 9, gi 0/1 - 2</i>
Set the port speed on the interface	<i>switch(config-if)#speed 10</i> <i>switch(config-if)#speed 100</i> <i>switch(config-if)#speed 1000</i> <i>switch(config-if)#speed auto</i>
Set the duplex mode on the interface	<i>switch(config-if)#duplex half</i> <i>switch(config-if)#duplex full</i> <i>switch(config-if)#duplex auto</i>
Enable or disable the interface	<i>switch(config-if)#no shutdown</i> <i>switch(config-if)#shutdown</i>
Show interface status of all ports	<i>switch#show interface status</i>
Show line and protocol status of all ports	<i>switch#show ip interface brief</i>

Be aware of the following switch configuration details:

- All switch ports are enabled (no shutdown) by default.
- Port numbering on some switches begins at 1, not 0. For example, **FastEthernet 0/1** is the first FastEthernet port on a 2960 switch.
- Through auto-negotiation, the 10/100/1000 ports configure themselves to operate at the speed of attached devices. If the attached ports do not support auto-negotiation, you can explicitly set the speed and duplex parameters.

- If the speed and duplex settings are set to **auto**, the switch will use auto-MDIX to sense the cable type (crossover or straight-through) connected to the port and will automatically adapt itself to the cable type used. When you manually configure the speed or duplex setting, it disables auto-MDIX so you will need to be sure to use the correct cable.
- The 2960 switch always uses the store-and-forward switching method. On other switch models, you might be able to configure the switching method.

3.5. Switch Interface Status

You can use the interface status to understand connectivity problems and quickly see whether the link between the device and the network is operational. Use the following commands to view the interface status:

Use...	To...
<code>switch#show interfaces</code>	List a large set of information about each interface.
<code>switch#show interface status</code>	View summary information about the interface status.
<code>switch#show ip interfaces</code>	View a small set of information about each IP interface.
<code>switch#show ip interfaces brief</code>	View a single line of information about each IP interface.

The following table summarizes some possible conditions indicated by the interface status for Ethernet interfaces:

Line status	Protocol status	Interface status	Indicates...
administratively down	down	disabled	The interface is administratively disabled with the shutdown command.
down	down	notconnect	<p>There is a hardware or network connection problem (Physical layer), such as:</p> <ul style="list-style-type: none">• No cable is connected.• The cable is connected but is improperly wired (or broken) so that signals cannot be sent or received correctly.• The device on the other end of the cable is powered off or the

			other interface is administratively shut down.
down	down	err-disabled	Port security has disabled the switch port.
up	up	connected	The interface is working correctly and a live connection is present.

© **Sergey Gorokhod**

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

3.6. TCP/IP Configuration

The following table summarizes many of the configuration settings for a TCP/IP network.

Parameter	Purpose
IP address	Identifies both the logical host and logical network addresses. Two devices on the same network must have IP addresses with the same network portion of the address.
Subnet mask	Identifies which portion of the IP address is the network address. Two devices on the same network must be configured with the same subnet mask.
Default gateway	Identifies the router to which packets for remote networks are sent. The default gateway address is the IP address of the router interface on the same subnet as the local host. Without a default gateway set, most clients will be unable to communicate with hosts outside of the local subnet.
Host name	Identifies the logical name of the local system.
DNS server	Identifies the DNS server that is used to resolve host names to IP addresses.
MAC address	Identifies the physical address. On an Ethernet network, this address is burned in to the network adapter hardware.

Note: A host requires an IP address and subnet mask to communicate on a single subnet. A default gateway address is required to enable inter-subnet communications. At least one DNS server address is required for the host to use hostnames when contacting other hosts.

Several of the TCP/IP configuration settings can be assigned through the following methods:

Method	Description
Dynamic Host Configuration Protocol (DHCP)	<p>A DHCP server is a special server configured to pass out IP address and other IP configuration information to network clients.</p> <ul style="list-style-type: none"> • The DHCP server is configured with a range of IP addresses it can assign to hosts. • The DHCP server can also be configured to pass out other IP configuration such as the default gateway and DNS server addresses. • The DHCP server ensures that each client has a unique IP address. • DHCP is a TCP/IP protocol. Any client configured to use DHCP can get an IP address from any server configured for DHCP, regardless of the operating system. <p>DHCP requires a DHCP server and minimal configuration.</p>
Automatic Private IP Addressing (APIPA)	<p>APIPA is a Microsoft implementation of automatic IP address assignment without a DHCP server. Using APIPA, hosts assign themselves an IP address on the 169.254.0.0 network (mask of 255.255.0.0).</p> <p>With APIPA:</p> <ul style="list-style-type: none"> • The host is configured to obtain IP information from a DHCP server (this is the default configuration). • If a DHCP server can't be contacted, the host uses APIPA to assign itself an IP address. • The host only configures the IP address and mask. It does not assign itself the default gateway and DNS server addresses. For this reason, APIPA can only be used on a single subnet. <p>Use APIPA as a fail-safe for when a DHCP server is unavailable to provide limited communication capabilities.</p>

Static assignment (manual)

Using static addressing, IP configuration information must be manually configured on each host. Use static addressing:

- On networks with a very small number of hosts.
- On networks that do not change often or that will not grow.
- To permanently assign IP addresses to hosts that must always have the same address (such as printers, servers, or routers).
- For hosts that cannot accept an IP address from DHCP.
- To reduce DHCP-related traffic.

Note: *Static addressing is very susceptible to configuration errors and duplicate IP address configuration errors (two hosts that have been assigned the same IP address). Static addressing also disables both APIPA and DHCP capabilities on the host.*

3.7. Switch IP Configuration

Keep in mind the following facts about IP addresses configured on switches:

- Basic switches operate at Layer 2, and therefore does not need an IP address to function. In fact, a switch performs switching functions just fine without an IP address set.
- You only need to configure a switch IP address if you want to manage the switch from a Telnet or Web session.
- The switch itself has only a single (active) IP address. Each switch port does *not* have an IP address (unless the switch is performing Layer 3 switching, a function which is not supported on all switches). The IP address identifies the switch as a host on the network but is not required for switching functions.

To configure the switch IP address, you set the address on the VLAN interface. This is a logical interface defined on the switch to allow management functions. By default, this VLAN is VLAN 1.

Use the following commands to configure the switch IP address:

```
switch#config terminal  
switch(config)#interface vlan 1  
switch(config-if)#ip address 1.1.1.1 255.255.255.0  
switch(config-if)#no shutdown
```

To enable management from a remote network, you will also need to configure the default gateway.

Use the following command in global configuration mode:

```
switch(config)#ip default-gateway 1.1.1.254
```

Note: You can use the **ip address dhcp** command to configure a switch (or a router) to get its IP address from a DHCP server. The DHCP server can be configured to deliver the default gateway and DNS server addresses to the Cisco device as well. The manually-configured default gateway address overrides any address received from DHCP.

3.8. Address Resolution Protocols

You should know the following protocols that perform address resolution.

Protocol	Description
Address Resolution Protocol (ARP)	Used by hosts to discover the MAC address of a computer from its IP address.
Reverse Address Resolution Protocol (RARP)	Used by a host to discover the IP address of a computer from its MAC address.
Bootstrap Protocol (BootP)	Used by a host (such as a diskless workstation) to query a bootstrap computer and receive an IP address assignment. A BootP server has a static list of MAC addresses and their corresponding IP addresses.
Dynamic Host Configuration Protocol (DHCP)	An improvement on BootP, DHCP is used to dynamically assign IP address and other TCP/IP configuration parameters. A DHCP server can use a static list to assign a specific IP address to a specific host. More commonly, however, the DHCP server automatically assigns an IP address from a preset range of possible addresses.

© Sergey Gorokhod

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

3.9. DHCP Configuration

Dynamic Host Configuration Protocol (DHCP) is a protocol used by hosts to obtain various parameters necessary for the clients to operate in a network. You can configure DHCP on a Cisco device through the command line interface (CLI) or the Security Device Manager (SDM).

DHCP configuration parameters include the following:

Component	Description
Address pool	The address pool is the range of addresses which can be assigned to requesting hosts. The DHCP server only assigns addresses within the address pool. The DHCP server can also be configured to not assign specific addresses in the range, known as exclusions .
Lease	The lease is the length of time for which the assignment is valid. It contains the assigned IP address and other information for the client. Periodically and when the client reboots, it contacts the DHCP server to renew the lease on the IP address.
DHCP options	In addition to the IP address and subnet mask, the DHCP server can also deliver the following: <ul style="list-style-type: none">• Domain Name Server (DNS) server address(s).• Default router (or default gateway) address.• Additional TCP/IP configuration parameters.
Binding	A binding is an association of a MAC address with a specific IP address . When you create a binding, the client with the specified MAC address is assigned the same IP address each time it requests an address. For example, if you have servers which should be accessible from outside the local network, the servers' IP addresses should remain the same. A binding is also known as DHCP reservation .
Interface	The interface that responds to DHCP requests is identified automatically according to the IP address assigned to the interface. When you configure the DHCP service on a Cisco device, it compares the subnet address specified in the address pool with the

	<p>IP addresses assigned to the router interfaces. If the interface has been assigned an IP address in the address pool, that interface will listen for and respond to DHCP requests.</p> <ul style="list-style-type: none"> • To allow an interface to listen and respond to DHCP requests, assign it an IP address within the address pool. If the interface does not have an IP address, or if the IP address is not within the address pool, client DHCP requests will be ignored. • You should exclude the interface IP address from the DHCP address pool.
--	--

A DHCP client uses the following process to obtain an IP address:

1. **Lease Request.** The client initializes a limited version of TCP/IP and broadcasts a **DHCPDISCOVER packet** requesting the location of a DHCP server.
2. **Lease Offer.** All DHCP servers with available IP addresses send **DHCP OFFER packets** to the client. These include the client's hardware address, the IP address the server is offering, the subnet mask, the duration of the IP lease, and the IP address of the DHCP server making the offer.
3. **Lease Selection.** The client selects the IP address from the first offer it receives and broadcasts a **DHCPREQUEST packet** requesting to lease the IP address in that offer.
4. **IP Lease Acknowledgment.** The DHCP server that made the offer responds and all other DHCP servers withdraw their offers. The IP addressing information is assigned to the client and the offering DHCP server sends a **DHCPACK (acknowledgement) packet** directly to the client. The client finishes initializing and binding the TCP/IP protocol.

The DHCP lease process uses frame-level broadcasts. For this reason, DHCP requests typically do not pass through routers to other subnets.

To enable DHCP across subnets:

- Enable BootP (DHCP broadcast) requests through the router.
- Configure a computer for BootP forwarding to request IP information on behalf of other clients.

3.10. DNS Services Commands

The following table describes the difference between a router and a workstation when resolving a logical host name to an IP address:

Device	Details
Router	<p>A router's DNS name resolution looks for information in the following places (in this order):</p> <ol style="list-style-type: none">1. Static DNS entries2. DNS server query (if enabled)
Workstation	<p>A workstation's DNS name resolution looks for information in the following places (in this order):</p> <ol style="list-style-type: none">1. Local DNS cache2. HOSTS file3. DNS server query (Primary)4. DNS server query (Secondary) <p>Note: Additional DNS servers are only consulted if the primary DNS server did not respond (i.e. it is offline).</p>

Use the following commands to configure DNS services on a router:

Use...	To...
<code>router(config)#ip host <name> a.b.c.d</code>	Create static DNS entries
<code>router(config)#ip domain-name <name></code>	Configure the router default domain
<code>router(config)#ip name-server a.b.c.d</code>	Set the default DNS name server
<code>router(config)#ip domain-lookup</code>	Enable the router to use DNS to identify IP addresses from host names
<code>router(config)#no ip domain-lookup</code>	Disable the broadcast name resolution of host names.
<code>router#show hosts</code>	Display a list of known IP hosts

3.11. Static and Default Route Commands

Most networks will use one (or more) routing protocols to automatically share and learn routes. Listed below are several situations when you might want to configure static routes.

- To configure a default route or a route out of a *stub* network (a stub network is one that has a single route into and out of the network).
- For small networks that do not change very often and that have only a few networks.
- To turn off all routing protocols and reduce traffic or improve security.
- To configure routes that is lost due to *route summarization*.

A *default route* is a route that is considered to match all destination IP addresses. With a default route, when a packet's destination IP address does not match any other routes, the router uses the default route for forwarding the packet.

Be aware of the following default route details:

- Default routes work best when only one path exists to a part of the network.
- One default route in the routing table could replace hundreds of static route entries in the routing table.
- When the default route is not set, the router discards packets that do not match a route in the routing table.

The following table lists the commands for configuring static routes:

Use . . .	To . . .
<i>Router(config)#ip route <destination> <next_hop></i>	Identify a next hop router to receive packets sent to the specified destination network.
<i>Router(config)#ip route <destination> <interface></i>	Identify the interface used to forward packets to the specified destination network.

<i>Router(config)#ip route 0.0.0.0 0.0.0.0 <next hop or interface></i>	Identify a default route to the specified destination network or through an interface. This is a method to set the <i>gateway of last resort</i> on a router.
<i>Router(config)#ip classless</i>	Enables the router to match routes based on the number of bits in the mask and not the default subnet mask.
<i>Router#show ip route</i>	View the routing table.
<i>Router#show ip route <hostname or address></i>	View details about the specific route.

Note: Configuring a static route to network 0.0.0.0 with mask of 0.0.0.0 is the most common method of configuring a default gateway. However, the following methods can also be used under certain circumstances:

- Use the ***ip default-network*** command to designate a route already in the routing table as the default route. For example, if the router had learned of network 10.0.0.0/8 through a routing protocol, you could use the following command to designate that network as the default network:
ip default-network 10.0.0.0
Be aware that the ***ip default-network*** command only makes a route a ***candidate*** for the default route, it does not necessarily guarantee that the route will be used to route packets to unknown destinations.
- Use the ***ip default-gateway*** command if IP routing has been disabled on the router. With IP routing disabled, routes will not be learned through a routing protocol, nor will static routes be used if configured. With IP routing enabled, the ***ip default-gateway*** setting will not be used.

Examples:

The following command creates a static route to network **192.168.1.0** through the router with the IP address **192.168.1.35** and gives it an administrative distance value of **25**:

Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.1.35 25

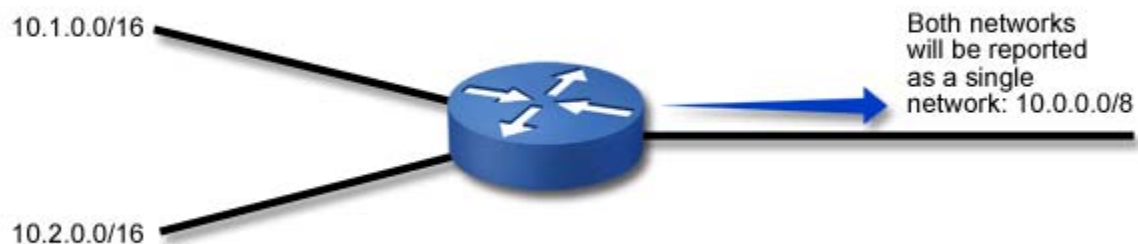
The following command identifies a default route through an interface with address **10.1.1.2**

Router(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2

Route Summarization

Process called **route summarization** to combine subnetted networks. The router identifies subnetted networks and combines them based on the default subnet mask.

For example, a router connected to networks **10.1.0.0/16** and **10.2.0.0/16** would combine the two networks into a single network **10.0.0.0/8**. This network would be reported to neighboring routers during routing exchanges.



© Sergey Gorokhod

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

3.12. RIP Commands

The **Routing Information Protocol (RIP)** is a simple, effective routing protocol for small- to medium-sized networks. By using a routing protocol, routers automatically share route information, reducing the amount of administration required for maintaining routes between networks.

To configure any routing protocol, use the following three steps:

1. Enable IP routing if it is not already enabled (use the **ip routing** command). By default, IP routing is already enabled, so this step is rarely required.
2. Switch to router configuration mode (use the **router** command, followed by the routing protocol you want to configure).
3. Identify the networks that will participate in dynamic routing (use the **network** command, followed by the address of a network to which the router is directly connected). This identifies the interfaces that will share and process received routing updates.
4. Configure any additional parameters based on the routing protocol.

The following table lists commands for configuring RIP.

Use . . .	To . . .
<i>Router(config)#ip routing</i>	Enable IP routing for the entire router. IP routing is enabled by default. Use this command only if it has been disabled. Use the <i>no ip routing</i> command to disable routing.
<i>Router(config)#router rip</i>	Enter router RIP configuration mode. Use the <i>no router rip</i> command to disable rip, removing all defined networks.
<i>Router(config-router)#version 2</i>	Enable RIP version 2 on the router.
<i>Router(config-router)#network <address></i>	Identify networks that will participate in the router protocol.

	<p>Notice that you identify <i>networks</i>, and not <i>interfaces</i>.</p> <p>When you use the network command to identify the networks that will participate in RIP routing, follow these rules.</p> <ul style="list-style-type: none"> • Identify only networks to which the router is directly connected. • Use the <i>classful</i> network address, not a subnetted network address. (The router will automatically convert a subnetted network address into a classful network address by removing subnetted network information.) <p>Use the <i>no network</i> command to remove any network entries.</p>
<i>Router#show ip route</i>	View the routing table.
<i>Router#show ip route <hostname or address></i>	View details about the specific route.

Example:

The following commands enable IP routing and identify two networks that will participate in the RIPv2 routing protocol.

```

Router(config)#ip routing
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.10.0

```


3.13. Routing Table

The router uses the routing table to determine where to send packets. When a packet is received, it compares the destination IP address contained in the packet with all known routes in the routing table.

- The destination address is compared to the networks in the routing table looking for a match.
- A match is made when the destination IP address is on the same subnet as indicated by the route in the routing table.
- The IP address might match more than one route in the routing table. If that is the case, the most specific routing table entry is used (i.e. the network with the subnet mask that has the greatest number of significant bits).
- When a match is found, the packet is sent out the specified router interface to the next hop router address.
- If no match is found, the packet is dropped (not forwarded).

Use the ***show ip route*** command to view the routing table. A sample output of this command is shown below.

```
Router1841#sh ip route
```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.2.1 to network 0.0.0.0

```
R 172.16.0.0/16 [120/1] via 192.168.1.1, 00:00:08, FastEthernet0/0
R 172.17.0.0/16 [120/2] via 192.168.1.1, 00:00:08, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0 [1/0] via 192.168.2.1
```

The following table describes important information shown in the command output:

Component	Description
Gateway of last resort	<p>The gateway of last resort identifies a route to use if the packet does not match any other route. In this example, the route of 0.0.0.0 with a mask of 0.0.0.0 matches every packet.</p> <p>If the destination IP address does not match any other route, the next hop address of 192.168.2.1 is used for this packet.</p> <p>Note: If the output shows the line Gateway of last resort is not set, then the router can only send packets to the specific routes listed in the routing table. Packets that do not match a specific route will be dropped.</p>
Route type	<p>The first character of a routing table entry identifies the source or type of the route.</p> <ul style="list-style-type: none">• C is for directly connected networks• S is for static routes• R is for routes learned through RIP• Additional codes indicate routes learned through other routing protocols <p>A route marked with * indicates a route that is a candidate for the default route. The router uses this route to determine whether the route can be used to set the gateway of last resort information.</p> <p>If it meets several conditions, the information in the route marked with * is used for the gateway of last resort information.</p>

Network	<p>Following the route type is the network address and subnet mask. This identifies the specific subnet address for the route.</p>
Administrative distance and cost	<p>The numbers in brackets following non-connected routes identify the following two items:</p> <ul style="list-style-type: none"> • The first number is the administrative distance. The administrative distance is a description of the trustworthiness or preference ability of a route learned from a specific source. Each source type (such as each routing protocol) is given a different administrative distance value. A lower number indicates a more preferred route. For example, a static route (AD = 1) is preferred over a route learned through RIP (AD = 120). • The second number is the cost to reach the route. The meaning of the route cost number is different depending on the source of the route, but generally it identifies how far away the destination is, either in distance or time. The cost is also referred to as the <i>metric</i>. The cost is only comparable when talking about routes learned from the same routing protocol. For example: <ul style="list-style-type: none"> ○ For two RIP routes, a cost of 1 indicates a lower-cost (shorter) route than a route with a cost of 2. ○ For a route learned through EIGRP, a cost of 312560 might identify a route that is faster than a route learned through RIP with a cost of 2. <p>Note: Be aware that the administrative distance is used to select a route learned between different protocols, while the cost is used to select the best route learned by the same protocol.</p>

Next hop router	<p>The address indicated by via identifies the router address where packets will be sent when sending to the destination network. The <i>next hop router address</i> is a router on the same subnet as a directly connected interface.</p> <p>However, this does not mean that the next hop router is connected directly to the destination network, but rather that it is the next stop in the path to the destination.</p>
Last update	<p>For routes learned through a routing protocol, the time value (such as 00:00:08) indicates the elapsed time since the last update about the route was received.</p> <p>Most protocols periodically send information about known routes.</p> <p>The update time helps you to know the <i>age of the route information</i>.</p>
Out interface	<p>The interface designation at the end of the route identifies the local router interface used to reach the next hop router and therefore to reach the destination network.</p>

Be aware of the following:

- Connected routes will only show if the interface has been assigned an IP address and is also up.
 - Static routes will only show if the interface used to reach the next hop router is up.
 - Having a route marked as a candidate default route does not necessarily mean that the router has a gateway of last resort set.
- To determine whether the router will route packets to unknown networks, examine the **Gateway of last resort** line for a next hop address.

3.14. ICMP Messages

The **Internet Control Message Protocol (ICMP)** is a special-purpose message mechanism added to the TCP/IP suite that lets computers and routers in internetwork report errors or provides information about unexpected circumstances. Remember that IP is a connectionless protocol and as such, contains no procedures that help to monitor successful packet delivery or test connectivity. Hosts use ICMP to send error messages to other hosts.

ICMP messages include the following types:

Message	Characteristics
Echo	The ICMP echo message is used to discover hosts and networks, and to verify that they are reachable. The ping utility is a popular utility that uses ICMP echo messages.
Destination unreachable	The destination unreachable message is sent if a packet cannot reach its destination for a variety of reasons. It might indicate the host is unavailable, or that there were problems detected in the packet header.
Time exceeded	The time exceeded message is sent when the packet's time-to-live (TTL) counter has expired.
Redirect	The redirect message is sent from a router to the sending device to indicate that a different route should be chosen for the packet. The redirect message can be sent if a better route is in the router's table, or if the selected route is unavailable or congested.
Source quench	The source quench message is sent by a receiving device to indicate that the flow of packets is too fast. When a sending device receives a source quench message, it slows its rate of transmission.
Router discovery	The router discovery message is a special broadcast message sent by hosts to discover the routers on a network. Routers respond to the message indicating their presence. They do not exchange routing information, but simply announce their availability.

3.15. TCP/IP Utilities

The following table describes three utilities you can use to test network connectivity between devices. You can use these utilities on Windows workstations as well as Cisco devices.

Utility	Description
Ping	<p>Ping sends an ICMP echo request/reply packet to a remote host. A response from the target device verifies that the host can communicate with the destination.</p> <ul style="list-style-type: none">• Ping operates at the Network layer.• A successful ping test verifies Network-layer connectivity between devices as well as the TCP/IP configuration of all devices in the path.• Ping reports success or failure, together with round-trip statistics.
Traceroute	<p>Traceroute uses ICMP echo request/reply packets together with the Time-to-Live (TTL) value in those packets to identify the path between two devices. Traceroute sends successive ICMP messages to a destination with increasing TTL values. For example, the first test pings the destination using a TTL of 1, the second pings with a TTL of 2, and so on.</p> <p>By default, traceroute sends three ping tests for each TTL value.</p> <ul style="list-style-type: none">• Traceroute operates at the Network layer.• Like ping, a successful test verifies Network-layer connectivity and TCP/IP configuration of devices in the path.• Traceroute reports success or failure for each hop in the path, along with the IP address and hostname (if available) of each hop. Statistics for each hop are also reported. <p>Note: On a Windows workstation, use the tracert command to perform a traceroute test.</p>

Telnet	<p>Telnet is an application that establishes a remote session with a destination device. For example, you use Telnet from a workstation or a Cisco device to create a remote console session with another device.</p> <ul style="list-style-type: none"> • Telnet operates at the Application layer. • A successful test verifies Application-layer connectivity. Because Telnet relies on lower-layer protocols, a successful Telnet session also verifies Network-layer and TCP/IP configuration. • A successful Telnet test opens a remote connection to the target device. <p>Note: <i>A successful Telnet test means that ping and traceroute will also be successful. A failed Telnet test only indicates a failure at the Application layer or below. By itself, it does not tell you at which layer the problem exists.</i></p>
--------	---

Be aware of the following when working with these utilities on Cisco devices:

- When using ping, an exclamation mark indicates a successful ping, while a period indicates a failure.
- Both ping and traceroute include a standard or an extended mode.
 - Extended mode is available only in privileged EXEC mode.
 - Use extended mode to modify the number of tests performed or the timeout period.
 - Use extended mode to test non-IP protocols (such as AppleTalk or Novell IPX).
- Responses to each test within the traceroute command are as follows:
 - A **time exceeded** message indicates that a router has received the packet but the TTL has expired. For example, if the TTL is set to 3, the third router in the path responds with the time exceeded message.
 - A **destination unreachable** message indicates that the router in the path does not have a route to the destination network or device, or the destination device is down.
 - An asterisk (*) indicates that the timer has expired without a response.

Note: The **time exceeded** and **destination unreachable** messages depend on the configuration of the intermediary and destination devices. Many devices are configured to not respond to ICMP messages, so you might see an asterisk even if the router in the path has received the packet.

- When using Telnet:
 - To suspend a Telnet session, press Ctrl + Shift + 6, then X.
 - To resume a Telnet session, use the **resume** command.
 - By default, debug information shows only on the console, not in the Telnet session window. Use the **terminal monitor** command to show debug information in a Telnet session.

3.16. Workstation TCP/IP Utilities

Using ping, tracert, and Telnet on a Windows workstation to test connectivity:

Utility	Description
Ipconfig	<p>Ipconfig displays IP configuration information for network adapters including:</p> <ul style="list-style-type: none">• IP address, mask and default gateway.• DNS and WINS server addresses.• IP address of the DHCP server used for configuration.• MAC address. <p>Use the ipconfig command as follows:</p> <ul style="list-style-type: none">• Use ipconfig to view IP address, subnet mask, and default gateway configuration• Use ipconfig /all to view detailed configuration information.• Use ipconfig /release to release the IP configuration information obtained from the DHCP server.• Use ipconfig /renew to request new IP configuration information from the DHCP server.
Arp	<p>The ARP cache keeps a mapping of IP address to MAC addresses. If the IP address or MAC addresses changes, the value in the cache might be out of date.</p> <ul style="list-style-type: none">• Use the arp -a to list a host's ARP cache.• Use arp -d to clear the ARP cache (remove all dynamic ARP entries from the ARP list). <p>Note: Switches used with arp are case-sensitive. Arp -a is not the same thing as arp -A.</p>
Nslookup	<p>Nslookup resolves (looks up) the IP address of a host name. Displays other name resolution-related information such as the DNS server used for the lookup request.</p>

3.17. IP Troubleshooting Tips

One important step in troubleshooting network communications is to verify the IP address, subnet mask, and default gateway settings of each host. Keep in mind the following as you troubleshoot IP:

- All computers must be assigned a unique IP address.
- Hosts on the same physical network should have IP addresses in the same address range.
- The subnet mask value for all computers on the same physical network must be the same.
- Configure the default gateway value to enable internetwork communication.
- The default gateway address must be on the same subnet as the host's IP address.
- You do not need to configure an IP address on a switch for frames to be switched through the switch. To ping to and from a switch or to remotely manage the switch, configure an IP address on the switch.

Listed below are several common symptoms and things to try to correct communication problems.

Problem	Symptoms	Solution
A single host cannot communicate with any other host.	Ping to any other host fails.	Because the problem exists with only one host, troubleshoot the configuration of the host with the problem.
A single host can communicate with all hosts on the same network, but can't communicate with any host on any other network.	Ping to hosts on the same network succeed, ping to hosts on other networks fails.	Verify the default gateway setting of the host with the problem. Because only a single host has the problem, you should be able to assume that the default gateway device is functioning correctly.
	Ping to hosts on the same network succeed, ping to hosts on other networks fails.	

<p>All hosts can communicate within the same network, but cannot communicate with any host outside of the local network.</p>	<p>Traceroute on the host times out with only a single entry.</p>	<p>Check for the following:</p> <ul style="list-style-type: none"> • If hosts have an IP address on the 169.254.0.0/16, then APIPA was used to assign the IP address and the default gateway value will be missing. Verify that the DHCP server is up. • If DHCP is used to assign IP information to hosts, verify the default gateway setting delivered by the DHCP server. • Verify that the default gateway device is up, has a valid connection to all networks, and has routing table information to reach destination networks.
	<p>Ping to the remote network fails, traceroute on the host times out with only a single entry.</p>	
<p>All hosts cannot communicate with hosts on a specific outside network. Communication with other networks is fine.</p>	<p>The routing table on the router does not show the destination network, or the gateway of last resort is not set.</p>	<p>Add a route to the routing table, or configure the gateway of last resort (default route) on the router. The gateway of last resort is also known as the default gateway for the router.</p>
	<p>The routing table has a route to the destination network. Traceroute on the router times out.</p>	

	Ping to the remote host fails. Traceroute to the remote host indicates no response from the host.	Troubleshoot other routers in the path to the destination network. Use traceroute to identify the last responding router and begin troubleshooting there.
All hosts cannot communicate with a specific remote host. Communication with other remote hosts in the same remote network is fine.	The routing table shows a route to the destination network (or the gateway of last resort is used).	Troubleshoot the configuration of the remote host.

3.18. LAN Segmentation

LAN segmentation is the process of dividing the network to overcome problems such as excessive **collisions**, **broadcast traffic**, or **heavy network traffic**. By segmenting a LAN, you can increase network performance, maximize bandwidth, and reduce congestion.

As you segment the network, you will need to consider the collision and broadcast domains on the network.

- A **collision domain** is any network or subnetwork where devices share the same transmission medium and where packets can collide. Collisions naturally increase as the number of devices in a collision domain increase.
- A **broadcast domain** is any network or subnetwork where computers can receive frame-level broadcasts from their neighbors. As you add devices to a network segment, the amount of broadcast traffic on a segment also increases.

Note: A special condition called a **broadcast storm** happens when broadcast traffic is sent, regenerated, and responded to. In this condition, the amount of broadcast traffic consumes network bandwidth and prevents normal communications. Faulty devices or improper configuration conditions can lead to a broadcast storm.

Segmentation may increase the number of both the collision and broadcast domains. Membership within collision or broadcast domains differs depending on the connection device used.

Device	Collision Domain	Broadcast Domain
Hub	All devices connected to the hub are in the same collision domain.	All devices are in the same broadcast domain.
Bridge or Switch	All devices connected to a single port are in the same collision domain (each port is its own collision domain).	All devices connected to the bridge or the switch is in the same broadcast domain.

Router	<p>All devices connected to a single interface are in the same collision domain.</p> <p>All devices accessible through an interface (network) are in the same broadcast domain. Each interface represents its own broadcast domain if the router is configured to not forward broadcast packets.</p>
---------------	---

In considering a network expansion solution, it is important to identify the connectivity problems you need to resolve, and then identify the device that is best suited for that situation. The main differences between routers, switches, and bridges are the range of services each performs and the OSI layer at which they operate.

Device	Characteristics
Router	<p>Routers perform the following functions that are not performed by bridges or switches.</p> <ul style="list-style-type: none"> • Route packets between separate networks • Modify packet size through fragmentation and combination • Route packets based on service address <p>Choose a router if you need to:</p> <ul style="list-style-type: none"> • Connect your network to a WAN, such as the Internet • Filter broadcast traffic to prevent broadcast storms • Connect two separate networks that use the same protocol • Improve performance in the event of a topology change (routers recover faster than bridges or switches) • Reduce the number of devices within a domain (effectively increasing the number of broadcast domains) • Enforce network security • Dynamically select the best route through an internetwork • Connect two networks of different architectures, for example Ethernet to Token Ring

Switch	<p>Choose a switch if you need to:</p> <ul style="list-style-type: none"> • Provide guaranteed bandwidth between devices • Reduce collisions by decreasing the number of devices in a collision domain (effectively creating multiple collision domains) • Implement full-duplex communication • Connect two network segments or devices using the same protocol • Provide improved performance over a current bridged network • Switch traffic without the cost or administration involved with routers
Bridge	<p>Choose a bridge if you need to:</p> <ul style="list-style-type: none"> • Isolate data traffic to one network segment • Route traffic from one segment to another (with the same network ID) • Link unlike physical media (e.g. twisted pair and coaxial Ethernet) of the same architecture type • Link segments that use the same protocol • Create segments without the expense and administration of routers <p>Note: <i>In most cases where you might use a bridge, choose a switch instead.</i></p>

In general, follow these guidelines to make decisions about the appropriate connectivity device.

- Use a bridge to segment the network (divide network traffic) and to provide fault tolerance.
- Use a switch to reduce collisions and offer guaranteed bandwidth between devices.
- Use a router to filter broadcast messages, implement security, or connect different networks.

LAN segmentation and design may be affected by the types of applications and protocols running over the network.

For instance, **Voice over Internet Protocol (VoIP)** requires a well-engineered, end-to-end network that provides little latency for data stream transmission. Fine-tuning the network to adequately support VoIP involves overcoming the following challenges:

- VoIP requires a very **low delay** as data is transferred between the sending and receiving phones, e.g. less than 200 milliseconds (.2 seconds).
- During transfer, the **jitter** (variations in delay) must be low as well, e.g. less than 30 milliseconds (.03 seconds).
- When packets do not arrive at the destination it is known as packet **loss**. If a VoIP packet was lost in transit, there is no need to recover the packet. This is because by the time the packet is recovered, it would sound like a break in the sound of the VoIP call.
- **Echo** is hearing your own voice in the telephone receiver while you are talking. When timed properly, echo is reassuring to the speaker; if the echo exceeds approximately 25 milliseconds, it can be distracting and cause breaks in the conversation. VoIP implementations use echo cancellers to regulate the echo.
- To secure VoIP data, the network should have a VoIP **Virtual Private Network (VPN)** solution. A VPN is a network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. Without a VoIP VPN solution, it is relatively easy to eavesdrop on VoIP calls and even change their content.
- In some cases, IP telephones require **Power over Ethernet (PoE)**. PoE is useful for powering IP telephones and other appliances where it would be inconvenient, expensive, or infeasible to supply power separately.

3.19. VoIP Considerations

Voice over IP (VoIP) is a protocol optimized for the transmission of voice through the Internet or other packet switched networks. Voice over IP protocols carry telephony signals as digital audio encapsulated in a data packet stream over IP.

VoIP requires a well-engineered, end-to-end network that provides little latency for data stream transmission. Fine-tuning the network to adequately support VoIP involves overcoming the following issues:

Issue	Description
Delay	<p>Delay (or <i>latency</i>) is the amount of time required for the spoken voice to be carried to the receiver's ear.</p> <ul style="list-style-type: none">• Delays cause long pauses between speaking and receiving, and might result in callers continually interrupting each other.• Callers notice roundtrip delays of 250 milliseconds (ms) or more.• International standards call for a delay of 150 ms or less.
Jitter	<p>Jitter is the variation of delay in transmissions.</p> <ul style="list-style-type: none">• Jitter causes strange sound effects as the delay of packets fluctuates.• Acceptable levels of jitter vary by vendor, but should be very low (between .5 and 30 ms).• Jitter can be controlled to some extent by packet buffers in VoIP equipment.
Packet loss	<p>Packet loss occurs when packets do not arrive.</p> <ul style="list-style-type: none">• Packet loss causes drop-outs in the conversation.• Because voice traffic is time sensitive, lost packets do not need to be retransmitted.• Voice traffic is very sensitive to packet loss. Even a 1% loss of packets can be detected.

	<ul style="list-style-type: none"> • Ideally, Cisco recommends 0% packet loss, although very low (.1-.5% maximum) might still be acceptable.
Echo	<p>Echo is hearing your own voice in the telephone receiver while you are talking.</p> <ul style="list-style-type: none"> • When timed properly, echo is reassuring to the speaker. • If echo exceeds approximately 25 milliseconds, it can be distracting and cause breaks in the conversation. • Excessive delay can cause unacceptable echo. • VoIP implementations use echo cancellers to regulate the echo.

VoIP is typically implemented using switches with additional configuration required on both switches and routers to ensure delivery of VoIP packets for acceptable quality.

- To minimize the number of switch ports required, VoIP phones connect to the switch port, and a corresponding workstation connects to the VoIP phone. Both voice and data traffic is sent through the same switch port.
- Switches with Power over Ethernet (PoE) capability provide electrical power through the Cat 5 cable. This eliminates the need to have a separate power cable for the phone.
- Switches and routers are configured with **Quality of Service (QoS)** settings to elevate the priority of voice traffic. This helps control delay and jitter.
- To secure VoIP data, the network should have a **VoIP Virtual Private Network (VPN)** solution. A VPN is a network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. Without a VoIP VPN solution, it is relatively easy to eavesdrop on VoIP calls and even change their content.